

## UNITED STATES DISTRICT COURT

APR 22 2019

for the  
Western District of Arkansas  
Fayetteville DivisionDOUGLAS F. YOUNG, Clerk  
By  
Deputy Clerk

In the Matter of the Search of )  
 Any and all structures and outbuildings to include )  
 vehicles located on the property or arriving )  
 on the property and curtilage of )  
 7688 Brooklyn Avenue )  
 Springdale, Arkansas 72762 )

Case No. 19 CM 45

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

**Any and all structures and outbuildings to include vehicles located on the property and arriving on the property and curtilage of 7688 Brooklyn Avenue, Springdale, Arkansas 72762, more particularly described on "Attachment A".**

**This court has authority to issue this warrant under 18 U.S.C. §§ 2703(c)(1)(A) and 2711(3)(A) and Federal Rule of Criminal Procedure 41**

The person or property to be searched, described above, is believed to conceal (*identify the person or describe the property to be seized*): **See "Attachment B"**

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of: **18 U.S.C. § 2252, et seq.**

The application is based on these facts: **See Affidavit of Task Force Officer Thomas Wooten- "Attachment C"**

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Thomas Wooten  
Applicant's signature

Thomas Wooten, Task Force Officer, HSI  
Printed name and title

Sworn to before me and signed in my presence.

Date: 4/21/19

Erin L. Wiedemann  
Judge's signature

City and state: Fayetteville, Arkansas

Erin L. Wiedemann, Chief United States Magistrate Judge  
Printed name and title

**ATTACHMENT A**

**PROPERTY TO BE SEARCHED:**

Any and all structures and outbuildings to include vehicles and campers located on the property or arriving on the property and curtilage of 7688 Brooklyn Avenue, Springdale, Arkansas 72762 (the **"SUBJECT PREMISES"**). The SUBJECT PREMISES is more particularly described as a one-story residence with a brick exterior, brown in color with white trim siding and facia. The numbers "7688" are affixed to the front of the home and to the right of the garage door. The residence is situated on the North side of Brooklyn Avenue with the front door facing South.



ATTACHMENT B  
ITEMS TO BE SEARCHED FOR AND SEIZED

- a. Images of child pornography and files containing images of child pornography in any form wherever it may be stored or found including, but not limited to:
  - i. Any computer, cellular phone, computer system, smart phones, computer tablets, and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, web cams, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to cellular telephones, hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;
  - ii. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
  - iii. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
  - iv. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
- b. Contact information or correspondence (online conversations/ Chats) pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, and/or the sexual solicitation of minors that were transmitted or received using a computer, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:
  - i. Electronic mail, internet chat logs, and electronic messages, social media messages, internet posts, blogs or any other internet-based contacts or communications, log in information to child exploitation forums, websites, and chatrooms;

- ii. Envelopes, letters, books, ledgers, diaries, notebooks, notes, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or the solicitation of sexual conduct;
- c. Emails, log in information, credit card information, etc showing ownership or use of the premises or device, subscriptions to internet or phone services, or account information and subscriptions to online applications known for child exploitation, paid sites, and social media;
- d. Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.
- e. Any and all computer hardware, to include data-processing devices containing central processing units, such as "desktop", "tower", "laptop" and "notebook" computers, hand-held electronic organizers, "personal digital assistants" and iPod's/iRiver's; "routers", "switchers" "Cellular Phones/Smart Phones" "Tablets" or any similar device which facilitates communication by sending transmissions to intended recipients and has the capability of creating logs; internal and external storage devices, including magnetic storage devices such as hard disk drives, diskette drives, and tape drives, optical storage devices such as CD-ROM drives, CD-R/CD-RW recorders, and DVD drives/recorders, and other memory storage devices such as smart-card readers. In addition, peripherals, equipment that send data to, or receive data from, computer hardware, but do not normally store user data, such as keyboards, mice, printers, scanners, plotters, video display monitors, modems, cables, and certain types of facsimile machines.
- f. Any and all computer software and storage media to include any material capable of storing information in a manner that can be used by computer hardware to save and/or retrieve information, such as diskettes, CD-ROM's, CD-R's, CD-RW's, DVD's, DVD-R's, DVD-RW's, magnetic tapes, ZIP disks, JAZ disks, Peerless disks, SparQ disks, ORB disks, optical disks, smart-cards, EPROMS, and digital memory media such as CompactFlash, SmartMedia, Sony Memory Sticks, and USB "thumb" or "key" drives, in addition to computer photographs, Graphic Interchange formats and/or photographs, cameras, digital cameras, slides, scanners or other visual depictions of such Graphic Interchange format equipment which may be, or are used to visually depict child pornography, child erotica, information pertaining to the sexual interest in children, sexual activity with children, or the distribution, possession or receipt of child pornography, child erotica or information pertaining to an interest in child pornography or child erotica.
- g. Any and all computer-related documentation to include written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items. In addition to passwords, to include alphanumeric strings, pass-phrases, password files, and similar decryption codes necessary to access data that is encrypted or otherwise inaccessible. Any and all security devices, to include physical keys, encryption devices, "dongles", and similar physical items needed to gain access to associated computer hardware.

h. Any and all address books, mailing lists, lists of names and addresses of minors, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States Mails or by computer, any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or minor contacted for sexual purposes.

i. Any data that is encrypted and unreadable will not be returned unless law Enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offense specified above.

j. In searching the data, the computer personnel may examine and copy all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized. In addition, the computer personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized. Finally, the computer forensic personnel may access any and all applications, email accounts, social media, and/or documents contained upon any said device to determine relevancy.

ATTACHMENT C

UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF ARKANSAS

STATE OF ARKANSAS

:  
:  
:  
:

ss. AFFIDAVIT

COUNTY OF WASHINGTON

Affidavit in Support of Application for Search Warrant

I, Thomas Wooten, a Task Force Officer with Homeland Security Investigations (HSI), being duly sworn, hereby depose and state as follows:

1. Since June 2000, I have been a police officer / detective with the Springdale, Arkansas Police Department. As such, I am authorized by the State of Arkansas to apply for and execute search warrants, arrest warrants and other instruments of the court. As a police officer / detective, I have received specialized training in matters related to criminal investigation, specifically but not limited to the area of sexual exploitation of minors, drug distribution, and money laundering. Since August of 2017, I have been assigned as a Task Force Officer to Homeland Security Investigations (HSI), a component of the U.S. Department of Homeland Security. As a Task Force Officer with HSI I primarily investigate crimes related to the sexual exploitation of minors. Prior to joining HSI, I attended a 40-hour training session covering Title 8, Title 18, Title 19 and Title 21 of the United States Code. As such, I am a law enforcement officer within the meaning of Section 115(c)(1) of Title 18 United States Code, who is authorized by law or Government agency to engage in or supervise the prevention, detection, investigation and/or prosecution of any violation of Federal and State criminal law.

2. This affidavit is being submitted in support of an application for a search warrant



for the premises located at 7688 Brooklyn Avenue, Springdale, Arkansas 72762 (hereinafter identified as the “**SUBJECT PREMISES**”). As such, it does not include all of the information known to me as part of this investigation, but only information sufficient to establish probable cause for the requested search warrant.

#### **Statutory Authority**

3. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors, which has been defined in Title 18 U.S.C. 2256, as an individual under 18 years of age.

a. Under 18 U.S.C. Section 2252(a)(1) (transportation), 2252(a)(2) (receipt and distribution), and 2252(a)(4)(B) and 2252A(a)(5)(B) (possession), it is a federal crime for any person to transport, distribute, receive, and possess child pornography, as that term is defined by federal law. Further under 18 U.S.C. Section 2253(a)(3), a person who is convicted of an offense under 18 U.S.C. Section 2252 or 2252A, shall forfeit to the United States such person’s interest in any property, real or personal, used or intended to be used to commit or to promote the commission of such offense.

#### **Computers and Child Pornography**

4. “Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable

costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership-base/subscription-based websites to conduct business, allowing them to remain relatively anonymous.

5. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that the development of computers has also revolutionized the way in which those who seek out child pornography are able to obtain this material. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by those who seek to obtain access to child pornography in these ways.

6. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store,



and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

7. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial Internet Service Providers (ISPs), such as America Online (“AOL”) and Microsoft, which allow subscribers to dial a local number and connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

8. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) websites that offer images of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by business, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient’s computer, including the Internet history and cache to look for “footprints” of the websites and images accessed by the recipient.

9. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a "hard drive") used in home computers has grown tremendously with the last several years. Hard drives with the capacity of 160 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

10. It should be noted that Internet Protocol (IP) numbers are unique identifiers leased to internet customers by their ISP's. Although IP numbers are capable of changing over time, only one (1) unique IP number can be assigned to a given customer's computer at any given time. Logs of these leased IP's (and their assigned customer accounts) are stored by ISP's routinely.

11. Your Affiant knows from his own experience and the training and experience of other law enforcement officers that Internet computers identify each other by an Internet Protocol or IP address. These IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead the law enforcement officer to a particular Internet service company and that company can typically identify the account that uses the address to access the Internet.

**Background Regarding Twitter Accounts**

12. Based on my knowledge and experience and information obtained from internet database queries and other law enforcement personnel with training and experience in this area, the following is known about Twitter, Incorporated accounts:

- a. Twitter is an online social networking service that enables users to send and read short 140-character messages called “tweets”. Registered users can read and post tweets, but those who are unregistered can only read them. Users access Twitter through the website interface or mobile device application.
- b. Twitter has become internationally identifiable by its signature bird logo. The original logo was in use from its launch in March 2006 until September 2010. A slightly modified version succeeded the first style when the website underwent its first redesign.
- c. Tweets are publicly visible by default, but senders can restrict message delivery to just their followers. Users can tweet via the Twitter website, compatible external applications (such as smartphones), or by short message services. Users may subscribe to other users tweets, this is known as “following” and subscribers are known as “followers”. Users can also “like” individual tweets. Twitter allows users to update their profile via their mobile phone either by text messaging or applications released for certain smartphones and tablets.
- d. Users can group posts together by topic or type by use of “hashtags”, words or phrases prefixed with a “#” sign. Similarly, the “@” sign followed by a username is used for mentioning or replying to other users. To repost a message from another Twitter user and share it with one’s own followers, a user can click

the retweet button within the tweet.

- e. Twitter has mobile applications for iPhone, iPad, Android, Windows 10, Windows Phone, BlackBerry, Firefox OS and Nokia S40. There is also versions of the website for mobile devices, SMS and MMS service.
- f. Individual tweets are registered under unique IDs using software called Snowflake, and geolocation data is added using Rockdove.
- g. Twitter messages are public, but users can also send private messages. Information about who has chosen to follow an account and who a user has chosen to follow is also public, though accounts can be changed to protected which limits this information and all tweets to approved followers.
- h. On June 1, 2011, Twitter announced its own integrated photo-sharing service that enables users to upload a photo and attach it to a tweet right from Twitter. Com. Users now also have the ability to add pictures to Twitter's search by adding hashtags to the tweet.

#### **Summary of the Investigation to Date**

13. On or around December 18, 2018 Your Affiant received a cybertip from the National Center for Missing and Exploited Children (NCMEC) in regards to images of child pornography being uploaded to a Twitter/Vine account. The Twitter account name was identified as Gary35133304 and was associated to a telephone number of (405) 413-2868. According to the cybertip, the user name Gary posted a comment stating, "Looking to trade underage links and pics." On or around November 25, 2018, four files containing images and videos of child pornography were uploaded to the Twitter/Vine account in question. The cybertip further stated,

“A NCMEC analyst has viewed the uploaded files and found what appears to be Apparent Child Pornography.”

14. Twitter, Incorporated provided the Cyber Tip Line with the following information of the user being reported:

Phone: +14054132868

Screen/User Name: Gary35133304

ESP User ID: 1066497618493231107

Profile URL: <https://twitter.com/Gary35133304>

IP Address: 45.26.84.70 (Registration) 11-25-2018 01:03:41 UTC

IP Address: 45.26.84.70 (Login) 11-25-2018 18:54:10 UTC

IP Address: 172.58.141.52 (Login) 11-25-2018 16:53:43 UTC

IP Address: 172.58.141.241 (Login) 11-25-2018 03:46:30 UTC

Number of Uploaded Files: 4

Full Name: Gary

Description: Looking to trade underage links and pics

15. On December 18, 2018, Your Affiant viewed the four uploaded files and found them to be four file folders containing multiple images and videos of pornography contained within the folders. The majority of the images of pornography depicted appeared to be prepubescent females that were completely naked with the camera focused primarily on their vaginas, breasts and buttocks or engaged in sexual acts. Your Affiant viewed two particular images located within the uploaded folders that were of concern to the ongoing investigation. On December 18, 2019, Your Affiant described two of these files as follows:

(a) **File Name: 1066509667470331909-F0iLYOhU**

This image depicted a white female between five to eight years of age, lying down and wearing a blue top with pink panties. She was lying on a bed with pink and red bedding material next to her.

The female was holding her panties to the side and exposing her vagina to the camera. The focus of the camera was on the child's exposed genitalia.

(b) **File Name: 1066565489399382020-rQA-tjHoGaSEsNCBly\_cF-GJjxtkqTSLu6c8fEvgZXs**

This video is approximately four second in length and depicted a prepubescent white female between the ages of five to eight years old being anally penetrated by an adult white males' penis. The female did not appear to have breast development or pubic hair.

16. On December 19, 2018, Your Affiant obtained and served ICE Summons# ICE-HSI-FU-2019-00066 to AT&T Internet Services, requesting account holder information for IP address 45.26.84.70. On January 30, 2019, Your Affiant obtained and served ICE Summons# ICE-HSI-FU-2019-00094 to T-Mobile, requesting account holder information for telephone number (405) 413-2868. On March 12, 2019, Your Affiant resubmitted the AT&T Internet Summons due to them not receiving the fax.

17. On March 06, 2019, Your Affiant received the requested summons information from T-Mobile and identified the owner of telephone number (405) 413-2868 as NICHOLAS C. BECKER (hereinafter identified as BECKER). Utilizing open source information as well as records from the State of Arkansas, Your Affiant was able to identify BECKER as follows:

NAME: NICHOLAS CHARLES BECKER

DATE OF BIRTH: August 29, 1996

RACE/SEX: White/Male

ADDRESS: 7688 Brooklyn Ave., Springdale, AR 72762

SSN (Last 4): 6596

ARKANSAS DRIVERS LICENSE (Last 4): 7366

18. On March 13, 2019, Your Affiant received the requested information from AT&T Internet services and identified the internet subscriber as HANNAH R. MACKEY (hereinafter



identified as MACKEY). Utilizing open source information as well as records from the State of Texas, Your Affiant was able to identify MACKEY as follows: (INVESTIGATORS NOTE: The address for BECKER and MACKEY was connected through utility information as well as BECKER'S listed address on his Arkansas Driver's License.)

NAME: HANNAH ROSE MACKEY

DATE OF BIRTH: June 17, 1998

RACE/SEX: White/Female

ADDRESS: 7688 Brooklyn Ave., Springdale, AR 72762

SSN (Last 4): 2188

TEXAS DRIVERS LICENSE (Last 4): 4407

19. On March 18, 2019 at approximately 1630 hours, Your Affiant conducted mobile surveillance at 7688 Brooklyn Avenue in Springdale, but did not observe any vehicles in the driveway. Your Affiant requested assistance from Springdale Police Detective Bobby Hammontree for the purpose of identifying vehicles at this address. On March 30, 2019 at approximately 12:30 hours, Detective Hammontree conducted mobile surveillance at 7688 Brooklyn Avenue in Springdale and identified a black Jeep Wrangler parked in the driveway. The black Jeep Wrangler displayed Texas license plate KZS7834, which returned to MACKEY.

20. On April 03, 2019 at approximately 05:45 hours, Your Affiant conducted mobile surveillance at the target address in Springdale and identified the previously reported Jeep parked in the driveway. Your Affiant also identified a gray Toyota Prius displaying Arkansas license plate 922SXJ parked in the driveway. The Toyota Prius was registered to Cynthia and Ronald Burns at 6002 S. 37<sup>th</sup> Street in Rogers, Arkansas 72758. Cynthia and Ronald Burns will not be further identified at this time. At approximately 06:15 hours, Your Affiant observed a white male with long hair exit the residence on Brooklyn Avenue and get in to the Toyota Prius. The male

was believed to be BECKER based on his build and long hair. The male then started his vehicle and then went back inside his residence. At approximately 06:30 hours, the same male and a female (believed to be MACKEY) left the address on Brooklyn Avenue, driving the Toyota Prius. Your Affiant followed the male and female to Wal-Mart Warehouse #8, located at 2100 SE 5<sup>th</sup> Street, Bentonville, Arkansas. At approximately 07:00 hours the female got out of the Toyota Prius and went inside of the business. Mobile surveillance was discontinued when the male subject left the parking lot.

21. Based on the information obtained at this point in the investigation, it is believed that BECKER and MACKEY cohabitate together at the "Subject Premises" in Springdale, Arkansas. The suspect IP address returned to MACKEY at the "Subject Premises" and the suspect telephone number returned to BECKER, as the cellular subscriber. BECKER'S listed address on his Arkansas driver's license returns to the "Subject Premises" and the water utility records are in MACKEY'S name at the "Subject Premises." Due to the information obtained thus far in the investigation, Your Affiant believes there is sufficient probable cause and requests a search warrant for the "Subject Premises."

### **Conclusion**

22. Based on my experience and the training and experience of other agents, many of the items sought in this affidavit may be stored electronically. Based on my experience and consultation with computer forensic experts, I know that electronic files can be easily moved from computer or electronic storage medium to another computer or medium. Therefore, electronic files downloaded to or created on one computer can be copied on or transferred to any other computer or storage medium at the same location. In addition, based on my experience, I know

that searching computerized information for evidence of crime often requires special agents to seize most or all of a computer system's central processing unit (CPU), input/output peripheral devices, related software, documentation, and data security devices, including passwords, so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:


(a) Volume of evidence: Computer storage devices such as hard disks, diskettes, tapes and laser disks, can store the equivalent of thousands of pages of information. This sorting process can take up to several months to complete, depending on the volume of data stored. Therefore, it would also be impractical to attempt this type of data search on site.

(b) Technical requirements: Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional destruction (both from external sources and from destructive code embedded in the system such as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

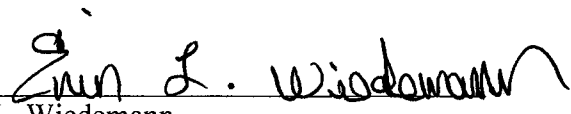
23. Therefore, authorization is sought in this application to seize the items set forth in attachment "B" that are found on the premises to be searched, in order to examine those items for evidence. If it is determined that data has been seized that does not constitute evidence of the crimes detailed herein, the government will return said data within a reasonable time.

24. Based on my experience and the training and experience of other agents involved with this investigation, your affiant knows that individuals involved in the sexual exploitation of children through child pornography almost always keep copies of their sexual explicit material. Among the reasons copies are maintained is because child pornography is illegal to openly purchase, and the most common method of acquiring it is by trading with other people with similar interests. It is also known that due to the inherent illegality of these sexually explicit materials, they are most often kept in a place considered secure, usually a residence, to avoid detection by law enforcement.

25. Based on the foregoing information, probable cause exists to believe there is located at 7688 Brooklyn Avenue, Springdale, Arkansas 72762, the SUBJECT PREMISES, for evidence of violations of Title 18, United States Code, Section 2252, et seq. Your Affiant prays upon his honorable court to issue a search warrant for the SUBJECT PREMISES for the items set forth in attachment "B" (which is attached hereto and incorporated herein by reference), that constitute evidence, fruits, and instrumentalities of violation of Title 18, United States Code, Section 2252, et seq.

  
\_\_\_\_\_  
Thomas Wooten, Task Force Officer  
Homeland Security Investigations

Affidavit subscribed and sworn to before me this 21st day of April 2019

  
\_\_\_\_\_  
Erin L. Wiedemann  
United States Magistrate Judge